Mangel an Cybersecurity-Fachkräften ist größte Herausforderung für MSPs

Sophos befragte MSPs in Nordamerika, Deutschland, Großbritannien und Australien nach dem Stand ihrer Cybersecurity

Wiesbaden, 29. Mai 2024 – Sophos hat heute seinen ersten „MSP Perspectives 2024“-Report zu den täglichen Herausforderungen bei der Cybersecurity für Managed Service Provider (MSPs) veröffentlicht. Die größte Herausforderung für MSPs besteht demnach darin, mit den neuesten Cybersecurity-Lösungen und -Technologien Schritt zu halten – 39 Prozent der befragten MSPs geben dies an. Darüber hinaus sind MSPs der Ansicht, dass eine weitere große Herausforderung die Einstellung neuer Cybersecurity-Fachkräfte ist, um mit dem Kundenwachstum und den neuesten Cyberbedrohungen Schritt zu halten,

Die Umfrage zeigt auch, dass MSPs den Mangel an internen Cybersecurity-Fähigkeiten als das größte Cybersecurity-Risiko sowohl für ihr eigenes Unternehmen als auch für die Kunden-Unternehmen ansehen. Auch gestohlene Zugangsdaten und Anmeldeinformationen sowie ungepatchte Schwachstellen gehören nach Ansicht der MSPs zu den größten Sicherheitsrisiken. So ergab etwa auch der jüngste Bericht Sophos State of Ransomware 2024, dass mit 29 Prozent fast ein Drittel der Ransomware-Angriffe mit kompromittierten Zugangsdaten beginnt, was die Prävalenz dieses Zugangsvektors zeigt.

„Die Geschwindigkeit der Innovation im Bereich der der Cybersecurity bedeutet, dass es für MSPs schwieriger denn je ist, mit den Bedrohungen und den Kontrollen, die diese stoppen sollen, Schritt zu halten. In Verbindung mit dem weltweiten Fachkräftemangel, der es vielen MSPs erschwert, Cybersecurity-Analysten zu finden und zu halten, überrascht es nicht, dass sich MSPs nicht in der Lage fühlen, mit der sich verändernden Bedrohungslandschaft Schritt zu halten", sagt Scott Barlow, Vice President of MSP bei Sophos. „Dies alles wird durch die Notwendigkeit einer 24x7-Abdeckung noch verstärkt, wie unser 2023 Active Adversary Report zeigt, der feststellt, dass 91 Prozent der Ransomware-Angriffe außerhalb der Geschäftszeiten stattfinden.“

Großteil der MSPs setzt auf Managed Detection and Response (MDR)

Als Reaktion auf diese komplexe Bedrohungslandschaft steigt die Nachfrage nach Managed Detection and Response (MDR)-Diensten, die eine permanente Abdeckung bieten. Derzeit bieten 81 Prozent der MSPs einen MDR-Dienst an. Mit 97 Prozent planen fast alle MSPs, die noch keinen MDR-Dienst anbieten, diesen im kommenden Jahr in ihr Portfolio aufzunehmen. Angesichts des Mangels an internen Cybersicherheitskompetenzen nutzen 66 Prozent der MSPs einen Drittanbieter für die Bereitstellung des MDR-Dienstes, und weitere 15 Prozent bieten ihn gemeinsam mit ihrem eigenen SOC und einem Drittanbieter an. Ganz oben auf der Liste der wichtigsten Fähigkeiten eines externen MDR-Anbieters steht bei MSPs die Fähigkeit, rund um die Uhr auf Vorfälle reagieren zu können.

Alle Cybersecurity Tools über eine Plattform zu organisieren, spart Arbeitsaufwand
Die Studie zeigt auch, dass mehr als die Hälfte (53 Prozent) der MSPs mit nur einem oder zwei Anbietern von Cybersicherheitslösungen arbeiten, während 83 Prozent der MSPs zwischen einem und fünf Anbieter nutzen. Angesichts des Aufwands und der Kosten, die mit dem Betrieb mehrerer Plattformen verbunden sind, schätzen MSPs, dass sie ihre tägliche Arbeitszeit um 48 Prozent reduzieren könnten, wenn sie alle ihre Cybersicherheitssysteme über eine einzige Plattform verwalten könnten.

Weitere Ergebnisse der Studie:

- 99 Prozent der MSPs berichten über eine steigende Nachfrage nach Unterstützung im Zusammenhang mit Cyber-Versicherungen. Dabei kommen die häufigsten Anfragen von Kunden, die einen MDR-Dienst implementieren möchten, um ihre Aussicht auf eine Versicherung zu verbessern (47 Prozent), oder jenen, die Hilfe beim Ausfüllen ihres Versicherungsantrags benötigen (45 Prozent).
- MSPs wünschen sich von ihrem MDR-Anbieter Flexibilität. 71 Prozent geben an, dass es „wichtig oder sehr wichtig“ ist, dass der Anbieter Telemetriedaten von ihren bestehenden Sicherheitstools für die Erkennung und Reaktion auf Bedrohungen nutzen kann.
- MSPs in den USA sind führend bei der Bereitstellung von MDR-Diensten: Fast alle (94 Prozent) bieten bereits MDR an. In Deutschland sind dies 70 Prozent, in Großbritannien 62 Prozent und in Australien 58 Prozent.

„Für MSPs ist es eine enorme Aufgabe, ihre Kunden vor schnelllebigen Cyberangriffen zu schützen. Wenn sie das richtige Sicherheits-Setup finden, dann haben sie aber hohe Chancen, ihr Geschäft und ihre Rentabilität zu steigern“, so Barlow. „Die Daten der Studie zeigen, dass MSPs ihr Angebot stärken und ihre Gemeinkosten senken, indem sie die von ihnen genutzten Plattformen zusammenlegen und sich mit MDR-Drittanbietern zusammenschließen, um ihr Serviceangebot zu erweitern. Beim Aufbau ihres zukünftigen Sicherheitsangebots sollten sie Anbietern den Vorzug geben, die ein komplettes Portfolio an branchenführenden, vollständig verwalteten Sicherheitsdiensten und -lösungen anbieten können.“

Über die Studie
Die Daten für den MSP Perspectives 2024 Report stammen aus einer anbieterunabhängigen Umfrage unter 350 MSPs in den USA (200), Großbritannien (50), Deutschland (50) und Australien (50). Die Umfrage wurde von Sophos in Auftrag gegeben und vom Marktforschungsunternehmen Vanson Bourne im März 2024 durchgeführt.

Der komplette Report inklusive der globalen und regionalen Daten und aufgeteilt nach Branchen steht unter MSP Perspectives 2024 bei Sophos.com bereit.

# # #

Social Media von Sophos für die Presse
Wir haben speziell für Sie als Journalist*in unsere Social-Media-Kanäle angepasst und aufgebaut. Hier tauschen wir uns gerne mit Ihnen aus. Wir bieten Ihnen Statements, Beiträge und Meinungen zu aktuellen Themen und natürlich den direkten Kontakt zu den Sophos Security-Spezialisten.

Folgen Sie uns auf und

LinkedIn: https://www.linkedin.com/groups/9054356/
X/Twitter: @sophos_info

Über Sophos
Sophos ist ein weltweit führender und innovativer Anbieter fortschrittlicher Lösungen zur Abwehr von Cyberangriffen, darunter Managed Detection and Response (MDR) sowie Incident Response Services. Das Unternehmen bietet ein breites Portfolio an Endpoint-, Netzwerk-, E-Mail- und Cloud-Sicherheitstechnologien, das bei der Abwehr von Cyberangriffen unterstützt. Als einer der größten auf Cybersecurity spezialisierten Anbieter schützt Sophos mehr als 600.000 Unternehmen und mehr als 100 Millionen Anwender weltweit vor aktiven Angriffen, Ransomware, Phishing, Malware und vielem mehr. Die Dienste und Produkte von Sophos sind über die cloudbasierte Management-Konsole Sophos Central verbunden und werden vom bereichsübergreifenden Threat-Intelligence-Expertenteam Sophos X-Ops unterstützt. Die Erkenntnisse von Sophos X-Ops erweitern das gesamte Sophos Adaptive Cybersecurity Ecosystem. Dazu gehört auch ein zentraler Datenspeicher, der eine Vielzahl offener APIs nutzt, die Kunden, Partnern, Entwicklern und anderen Anbietern von Cybersecurity und Informationstechnologie zur Verfügung stehen.
Sophos bietet Cybersecurity-as-a-Service für Unternehmen an, die vollständig verwaltete, schlüsselfertige Sicherheitslösungen benötigen. Kunden können ihre Cybersecurity auch direkt mit der Security Operations Platform von Sophos verwalten oder einen hybriden Ansatz verfolgen, indem sie ihre internen Teams mit Sophos Services ergänzen, einschließlich Threat Hunting und Systemwiederherstellung. Sophos vertreibt seine Produkte über Reseller und Managed Service Provider (MSPs) weltweit. Der Hauptsitz von Sophos befindet sich in Oxford, U.K.
Weitere Informationen unter: www.sophos.de

Pressekontakt:

Sophos
Jörg Schindler, Senior PR-Manager EMEA Central
joerg.schindler@sophos.com, +49-721-25516-263

TC Communications
Arno Lücht, +49-8081-954619
Thilo Christ, +49-8081-954617
Ulrike Masztalerz, +49-30-55248198
Ariane Wendt +49-172-4536839
sophos@tc-communications.de